Modification no 9 de la SPD de préqualification - IaaS et PaaS native

Nº de sollicitation :	CS-IAAS-2024.	Modification : 009

Cette modification a pour but :

1. De fournir des réponses aux questions reçues, décrites en détail dans la section A.
2. De fournir la version la plus à jour de la pièce jointe 1 – Grille d'évaluation de la préqualification, comprenant toutes les modifications qui ont été faites, comme indiqué en détail dansla section B.

Section A - Questions et réponses (série nº 7)

	Question	Réponse
103	En réponse à une question récente, la Couronne a révisé l'exigence selon laquelle les soumissionnaires doivent respecter trois des cinq principes de confiance du SOC 2 Type II de l'AICPA. La cinquième exigence, à savoir la protection de la vie privée, a été ajoutée à la suite de cette modification récente. Bien que les exigences du SOC 2 Type II de l'AICPA évaluent un large éventail de contrôles relatifs à la sécurité des données, y compris la confidentialité et la protection de la vie privée, dans ce contexte, de nombreux fournisseurs de services infonuagiques choisissent d'adhérer à la norme ISO 27018 et de se certifier par rapport à celle-ci, car il s'agit d'une norme plus rigoureuse qui s'applique spécifiquement aux déploiements en nuage. La norme ISO 27018 est une norme spécifique pour les fournisseurs de services infonuagiques (FSI) qui se concentre sur la protection des informations personnelles identifiables (PII) dans le nuage. Elle fournit des conseils et des contrôles pour le traitement des PII, en abordant des questions telles que le traitement des données, la transparence,	À cette étape du processus de préqualification, le Canada ne modifiera pas les critères de préqualification, mais examinera votre proposition pour une étape ultérieure de ce processus d'approvisionnement.

	le consentement et la conformité avec les lois et réglementations applicables en matière de protection de la vie privée. Alors que la norme SOC 2 Type II comprend des contrôles relatifs à la protection et à la confidentialité des données, qui répondent indirectement aux préoccupations en matière de protection de la vie privée, la norme ISO 27018 propose un ensemble de contrôles spécifiques adaptés aux fournisseurs de services en nuage pour protéger les PII dans un environnement en nuage. Elle comprend des dispositions relatives au cryptage des données, aux contrôles d'accès, à la portabilité des données, à la transparence et au respect des exigences légales et réglementaires en matière de protection de la vie privée. Compte tenu du fait que la Couronne souhaite que les fournisseurs qualifiés respectent trois des cinq principes de confiance liés à la sécurisation des données du Canada et que ce processus de préqualification concerne spécifiquement les solutions basées sur l'informatique en nuage, la Couronne considérera-t-elle la certification ISO 27018 comme un équivalent satisfaisant (voire une norme plus rigoureuse) pour le respect de la norme relative à la protection de la vie privée et de la confidentialité ?	
104	En ce qui concerne les réponses du Canada à la question numéro 93 de la modification 008 – La réponse a entraîné une certaine confusion quant à la notation basée sur les différentes étapes du processus du PVMC. Nous demandons au Canada de confirmer que tous les points seront attribués si le module se trouve à l'étape de la « COORDINATION » du processus du PVMC. La modification stipule que les points complets ne seront attribués que si le module est en cours d'examen (c'est-à-dire à l'étape 3). Cependant, le statut de « coordination » est en fait l'étape 4 du processus qui est au-delà du statut « étape 3 en cours d'examen » et devrait donc recevoir tous les points selon notre compréhension.	Comme indiqué précédemment, les critères restent inchangés après l'amendement 8. L'exigence spécifique est que le soumissionnaire « ait fourni un module ayant atteint ou dépassé le statut "En cours de révision" pour la validation FIPS 140-3 dans la liste des modules en cours de traitement par la PVMC à la date de clôture de la CBS pour la préqualification ». Conformément au déroulement du processus de validation du PVMC, les statuts qui suivent « En cours d'examen » sont « Coordination » et « Finalisation ». Par conséquent, un module dont le statut est « En cours d'examen », « Coordination » ou « Finalisation » reçoit 3 points.

Section B

À toutes fins utiles, le Canada fournit la dernière version de la pièce jointe 1 - Grille d'évaluation de la préqualification, qui comprend toutes les modifications qui ont été apportées à ce jour.

Partie A – Critères obligatoires

Les critères obligatoires suivants doivent être satisfaits.

	Critères	Renseignements devant être fournis par les soumissionnaires	Éléments de notation
O1	**Capacité du soumissionnaire à vendre une infrastructure en tant que service (IaaS) disponibles sur le marché ET une plateforme en tant que service (PaaS).** Le soumissionnaire doit être un fournisseur de services infonuagiques (FSI) proposant des services d'IaaS disponibles sur le marché **ET** des services de PaaS native. Aux fins de cette sollicitation, un type d'instance, dans le contexte de l'informatique en nuage, fait référence à une machine virtuelle proposée par les fournisseurs de services cloud.	Le soumissionnaire devrait fournir les URLs actuellement accessibles au public énumérant les services d'IaaS disponibles sur le marché et les services de PaaS native suivants : 1. les services (types d'instances) qui répondent à chaque catégorie des services d'IaaS disponibles sur le marché : a. Catégorie 1 – Instances à usage général ou standard qui peuvent être configurées de façon à équilibrer la quantité de ressources de calcul, mémoire et réseau en fonction des exigences des applications et des charges de travail. b. Catégorie 2 – Instances optimisées pour le calcul pour les applications et les charges de travail qui exigent une grande puissance de calcul utilisant des processeurs haute performance. c. Catégorie 3 – Instances à mémoire optimisée pour les applications et les charges de travail qui exigent un traitement rapide de grands ensembles de données en mémoire. d. Catégorie 4 – Instances spécialisées pour les applications et les charges de travail qui nécessitent des exigences particulières, y compris n'importe qu'elles des sous-catégories suivantes : i. Calcul de haute performance (CHP) ii. Capacités de stockage accrues iii. Processus assisté par GPU (unité centrale graphique) iv. Systèmes d'apprentissage automatique e. Catégorie 5 – Capacités évolutives de stockage de blocs, d'objets et de fichiers	Pour être conforme, le soumissionnaire doit démontrer les services suivants par le biais des URLs actuellement accessibles au public : • Un minimum de 5 services d'IaaS disponibles sur le marché pour chacune des catégories de 1 à 4, démontrés par leur liste de produits/services publiquement visible (1a à 1d). • Un minimum de 3 services d'IaaS disponibles sur le marché pour la catégorie 5, démontrés par sa liste de produit/service publiquement visible (1e). • Un minimum de 1 service d'IaaS disponibles sur le marché pour chacune des catégories 6 et 7, démontrés par leur liste de produits/services publiquement visible (1f et 1g). • Un minimum de 4 services de PaaS disponibles sur le marché pour chacune des catégories, démontrés par leur liste de produits/services publiquement visible (2a à 2f). Le soumissionnaire doit fournir une adresse URL actuellement accessible au public comme preuve directe de l'exigence. Veuillez noter que le Canada n'ira pas au-delà de cette URL en aucune circonstance

	Critères	Renseignements devant être fournis par les soumissionnaires	Éléments de notation
		f. Catégorie 6 – Stockage hors-ligne pour le stockage à long terme de données archivées g. Catégorie 7 – Stockage de haute performance fondé sur la technologie de disque SSD (disque statique à semiconducteurs). 2. les services (types d'instances) qui répondent collectivement à chaque catégorie des services de PaaS native suivants : a. Catégorie 8 - Services de conteneurs b. Catégorie 9 - Outils du développeur c. Catégorie 10 - Services de bases de données d. Catégorie 11 - Services réseau et de sécurité e. Catégorie 12 - Intelligence artificielle (IA) ou apprentissage automatique f. Catégorie 13 - Services d'analyse et de métadonnées.	
O2	**Capacité du soumissionnaire à sécuriser les données du Canada** Le soumissionnaire doit détenir les dernières versions des certifications de l'industrie et rapports de vérification actuels et valides suivants : 1. Norme ISO/IEC 27001 : Technologie de l'information – Techniques de sécurité – systèmes de gestion de la sécurité de l'information – Exigences ; 2. Norme ISO/IEC 27017 : Technologie de l'information – Techniques de sécurité – Code de pratique pour les contrôles de la sécurité de l'information fondés sur la norme ISO/IEC 2 7002 en ce qui concerne les services infonuagiques ; 3. Norme Service Organization Control (SOC) 2 Type II de l'AICPA pour un minimum de 3 des 5 principes de confiance suivant : de sécurité, de disponibilité, d'intégrité du traitement, de protection de la vie privé et de confidentialité. *Seules les certifications émises par une tierce partie indépendante admissible en vertu de l'AICPA, CPA Canada ou conformément à la norme de système de qualité ISO/IEC 17020 seront acceptées.	Le soumissionnaire devrait fournir les évidences suivantes : - Pour chaque certification : des copies des certifications et des rapports de vérification incluant la date d'émission et d'expiration (le cas échéant). Si une certification a expiré ou doit expirer avant la date de clôture de la SPD pour la préqualification et que le soumissionnaire est dans le processus de renouvellement, une lettre de vérification ou une déclaration de l'organisme émetteur confirmant l'état actuel et valide de la certification doit être fournie. - Pour SOC2 : Copies des rapports de vérification, les principes de confiance, la date d'émission et d'expiration (le cas échéant).	Pour être conforme, le soumissionnaire doit démontrer qu'il possède : a) les dernières versions des certifications et rapports de vérification actuels, et valides suivants : norme ISO/IEC 27001 et la norme ISO/IEC 27017 ; b) norme service Organization Control (SOC) 2 Type II de l'AICPA qui inclue un minimum de 3 des principes de confiance suivant : • sécurité • disponibilité • intégrité du traitement • protection de la vie privé • confidentialité.

	Critères	Renseignements devant être fournis par les soumissionnaires	Éléments de notation

Partie B – Critères cotés

Les critères suivants seront cotés selon les éléments de notation définis dans le tableau.

Note totale maximale = 77 points

	Critères	Renseignements à fournir par les soumissionnaires	Éléments de notation
C1	**Capacité à satisfaire les exigences en matière d'hébergement (maximum 15 points)** Le soumissionnaire devrait avoir au moins deux centres de données situées dans une seule et même région au Canada. Le Canada utilise le système de classification par niveaux de l'Uptime Institute pour la définition des centres de données. Aux fins de cette sollicitation, un centre de données (CD) est une infrastructure physique qui répond ou dépasse les exigences du niveau « Data Center Tier III ». Un CD fait partie d'une région. Une région est définie comme étant plusieurs centres de données situés à moins de 100 km les uns des autres dans la même région définie. Un centre de données fait partie de l'offre de services infonuagiques disponible publiquement sur le marché du soumissionnaire.	Le soumissionnaire devrait fournir l'adresse physique de 2 centres de données situées dans la même région au Canada. Si le soumissionnaire choisit de ne pas fournir l'adresse physique, il peut fournir : • la désignation publique de chaque centre de données du soumissionnaire ; • le code postal complet ; • la distance directe (en km) entre les centres de données.	Jusqu'à 15 points seront attribués. Les points seront attribués comme suit : **15 points :** Le soumissionnaire a fourni les adresses physiques ou les codes postaux de 2 centres de données situées dans la même région au Canada = 15 points ; **10 points :** Le soumissionnaire a fourni les adresses physiques ou les codes postaux de 2 centres de données mais ils ne sont pas situés dans la même région au Canada = 10 points ; **5 points :** Le soumissionnaire a fourni l'adresse physique ou le code postal de 1 centre de données situées au Canada = 5 points ; **0 point :** Le soumissionnaire n'a pas fourni l'adresse physique ou le code postal d'un centre de données situées au Canada = 0 point.
C2	**Capacité de la solution du soumissionnaire à protéger les données du Canada (maximum 12 points)** Le soumissionnaire devrait démontrer que la solution la capacité de chiffrer les données en transit et au repos en utilisant la cryptographie approuvée par le Centre de la sécurité des télécommunications Canada (CST).	**Dans le cas des données en transit :** Pour démontrer sa capacité, le soumissionnaire devrait fournir un mécanisme cryptographique utilisé pour empêcher la divulgation non autorisée de renseignements et pour détecter toute modification apportée aux renseignements durant la transmission et fournir des preuves des éléments suivants :	Jusqu'à 12 points seront attribués. **1. <u>Dans le cas des données en transit</u> :** Les points seront attribués comme suit : a) Module cryptographiques : **3 points :** Le soumissionnaire a fourni un numéro de certificat qui démontre que le module est confirmé FIPS 140-3 en vertu du PVMC ou un module qui est

	Critères	Renseignements à fournir par les soumissionnaires	Éléments de notation
	La cryptographie approuvée par le CST se trouve sur la page suivante : Algorithmes cryptographiques pour l'information NON CLASSIFIÉE, PROTÉGÉ A et PROTÉGÉ B - ITSP.40.111 (version 3 – 18 mars 2024) (https://www.cyber.gc.ca/fr/orientation/algorithmes-cryptographiques-linformation-non-classifie-protege-protege-b-itsp40111) et Conseils sur la configuration sécurisée des protocoles réseau (ITSP.40.062) - Centre canadien pour la cybersécurité (révision 2 – 13 octobre 2020) https://www.cyber.gc.ca/fr/orientation/conseils-sur-la-configuration-securisee-des-protocoles-reseau-itsp40062) *Remarque à l'intention des soumissionnaires : Cette exigence n'est pas obligatoire à l'étape de la présélection. Dans les phases ultérieures du processus d'approvisionnement, nous exigerons tous les mécanismes cryptographiques ainsi que les modules et algorithmes utilisés, et ils seront vérifiés avant l'attribution du contrat.*	a) Déterminer si la conformité d'un module cryptographique à la norme FIPS 140-3 a fait l'objet d'essais et été validée en vertu du Programme de validation des modules cryptographiques (PVMC) ou est en cours d'examen : Exigences de sécurité pour les modules cryptographiques (Security Requirements for Cryptographic Modules) conformément à l'article 12 de la norme ITSP 40.111 Pour un module confirmé : le soumissionnaire devrait fournir le nom du module et le numéro de certificat Pour un module en cours d'examen : Le soumissionnaire devrait fournir le nom du module et le statut de validation selon la liste des Modules en processus de validation par le CMVP, pour la validation FIPS 140-3. b) Déterminer un algorithme de chiffrement qui a été mis en œuvre et confirmer qu'il fait partie de la liste d'algorithmes de chiffrement recommandés conformément aux articles 2 et 3 de la norme ITSP 40.111 et le tableau correspondant de l'ITSP 40.062. Le soumissionnaire devrait fournir le nom de l'algorithme ainsi que le tableau correspondant de l'ITSP.40.062. c) Confirmer si la mise en œuvre de l'algorithme cryptographique a été soumise à des essais et validées en vertu du Programme de validation des algorithmes cryptographiques (CAVP pour Cryptographic Algorithm Validation Program), conformément à l'article 12 de la norme ITSP 40.111. Le soumissionnaire devrait fournir le numéro de validation. **2. Dans le cas des données au repos :**	minimalement à l'étape « En cours d'examen » (In review) dans la liste des Modules en processus de validation pour la validation FIPS 140-3 en vertu du PVMC à la date de clôture de la SPD de préqualification. **1 point :** Le soumissionnaire a fourni un numéro de certificat qui démontre que le module est confirmé à FIPS 140-2, en vertu du PVMC. **0 point :** Non confirmé FIPS en vertu du PVMC. b) L'algorithme de chiffrement : **2 points :** L'algorithme de chiffrement mis en œuvre figure dans l'un de tableaux (Tableaux 1 à 21) sous la colonne « recommandé » dans l'ITSP.40.062. **1 point :** L'algorithme de chiffrement mis en œuvre figure dans l'un de tableaux (Tableaux 1 à 21) sous la colonne « suffisant » dans l'ITSP.40.062. **0 point :** Tout autre algorithme qui ne figure pas dans l'un des tableaux sous les colonnes recommandée et suffisante dans l'ITSP.40.062 c) Algorithme cryptographique : **2 points :** Le soumissionnaire a fourni un numéro de validation qui démontre que l'algorithme cryptographique est validé en vertu du CAVP. **0 point :** Le soumissionnaire n'a pas fourni un numéro de validation qui démontre que l'algorithme cryptographique est validé en vertu du CAVP. **2. Dans le cas des données au repos :** Les points seront attribués comme suit : a) Module cryptographiques : **3 points :** Le soumissionnaire a fourni un numéro de certificat qui démontre que le module est confirmé FIPS 140-3 en vertu du PVMC ou un module qui est minimalement à l'étape « En cours d'examen » (*In review*) dans la liste des Modules en processus de validation pour la validation FIPS 140-3 en vertu du

	Critères	Renseignements à fournir par les soumissionnaires	Éléments de notation
		Pour démontrer sa capacité, le soumissionnaire devrait fournir un mécanisme cryptographique utilisé pour empêcher la modification et la divulgation non autorisées de renseignements au repos sur les composants du système d'information stockant les données du Canada et fournir des preuves des éléments suivants : a) Déterminer si la conformité d'un module cryptographique à la norme FIPS 140-3 a fait l'objet d'essais et été validée en vertu du Programme de validation des modules cryptographiques (PVMC) ou est en cours d'examen : Exigences de sécurité pour les modules cryptographiques (Security Requirements for Cryptographic Modules) conformément à l'article 12 de la norme ITSP 40.111 Pour un module confirmé : le soumissionnaire devrait fournir le nom du module et le numéro de certificat Pour un module en cours d'examen : Le soumissionnaire devrait fournir le nom du module et le statut de validation selon la liste des Modules en processus de validation par le CMVP, pour la validation FIPS 140-3. b) Confirmer si la mise en œuvre de l'algorithme cryptographique a été soumise à des essais et validées en vertu du Programme de validation des algorithmes cryptographiques (CAVP pour Cryptographic Algorithm Validation Program), conformément à l'article 12 de la norme ITSP 40.111. Le soumissionnaire devrait fournir le numéro de validation.	PVMC à la date de clôture de la SPD de préqualification. **1 point :** Le soumissionnaire a fourni un numéro de certificat qui démontre que le module est confirmé à FIPS 140-2, en vertu du PVMC. **0 point :** Non confirmé FIPS en vertu du PVMC. b) Algorithme cryptographique : **2 points :** Le soumissionnaire a fourni un numéro de validation qui démontre que l'algorithme cryptographique est validé en vertu du CAVP. **0 point :** Le soumissionnaire n'a pas fourni un numéro de validation qui démontre que l'algorithme cryptographique est validé en vertu du CAVP.
C3	**Expérience du soumissionnaire à fournir des services d'IaaS et de PaaS native à de grandes organisations (maximum 21 points)** Le soumissionnaire devrait démontrer son expérience	Pour démontrer son expérience, le soumissionnaire devrait fournir une liste de trois (3) clients à qui des services d'IaaS et de PaaS native ont été offerts.	Jusqu'à 21 points seront attribués en utilisant la moyenne des points totaux pour les trois clients. Les points seront attribués comme suit : **Durée des services fournis au client**

	Critères	Renseignements à fournir par les soumissionnaires	Éléments de notation
	en matière de fourniture de services d'IaaS et de PaaS native à de grandes organisations gouvernementales ou à de grandes sociétés privées externes. *« externe » fait référence aux organisations ou aux sociétés qui ne font pas partie de la propre structure d'entreprise du soumissionnaire ou de son organisation mère.* *Dans ce critère, « services uniques » désigne un élément spécifique du catalogue de services infonuagiques publics et disponibles sur le marché. Cela exclut spécifiquement les services infonuagiques non publics, y compris, mais sans s'y limiter, les services infonuagiques privés et les services d'hébergement de centre de données.*	Pour chaque client, les renseignements suivants devraient être fournis : 1) Le nom de l'entreprise cliente 2) La durée des services, y compris la date de début et de fins des services (mois et année) 3) Le nombre d'employés de l'entreprise cliente 4) Le nombre de services uniques fournis et utilisés par le client au cours de la durée des services.	**7 points :** 7 ans ou plus **5 points :** 5 ans ou plus et moins de 7 ans **3 points :** 3 ans ou plus et moins de 5 ans **0 point :** Moins de 3 ans **Nombre d'employés du client** **7 points :** 50 000 employés ou plus **5 points :** Entre 29 999 et 50 000 employés **3 points :** Entre 9 999 et 30 000 employés **0 point :** Moins de 10 000 employés **Services uniques fournis et utilisés** **7 points :** 200 services et plus **5 points :** Entre 149 et 200 services **3 points :** Entre 99 et 150 services **0 point :** Moins de 100 services Si plus de trois clients sont présentés, seuls les trois premiers clients inscrits dans la soumission seront évalués.
C4	**Capacité du soumissionnaire à répondre aux besoins du Canada (maximum de 29 points)** Le soumissionnaire devrait démontrer sa capacité à répondre aux besoins du Canada.	Le soumissionnaire devrait fournir les renseignements suivants afin de démontrer sa capacité à répondre aux besoins du Canada pour chaque élément énuméré ci-dessous : **Évaluation comparative** 1. Le nombre de régions au Canada. 2. Le nombre de régions mondialement. 3. Le nombre de centres de données (CD) au Canada. Le soumissionnaire devrait fournir la ville de chaque CD associé à la région. 4. Le nombre total de centres de données déployés et en service mondialement. 5. Le nombre de points d'échange Internet au Canada. Le soumissionnaire devrait fournir le nom des entreprises de chaque fournisseur de points d'échange Internet avec lequel il est associé. 6. Le nombre de points d'échange Internet mondialement	Jusqu'à 29 points seront attribués en utilisant la somme de l'évaluation comparative et la notation directe des éléments (1 à 11). Chaque élément (1 à 11) se verra attribuer des points individuellement. **Évaluation comparative des éléments** Pour les éléments 1 à 9 : A. **Établissement du classement** : Les soumissionnaires seront classés du nombre le plus élevé au nombre le plus bas. B. **Attribution des points** : Les points seront attribués en fonction du classement du soumissionnaire dans chaque élément, du plus élevé au plus bas. Les points seront attribués pour chaque élément de comparaison comme suit : **3 points :** Soumissionnaire classé premier **2 points :** Soumissionnaire classé deuxième **1 point :** Soumissionnaire classé troisième **0 point :** Autres soumissionnaires classés (4e position et plus) **Notation directe**

	Critères	Renseignements à fournir par les soumissionnaires	Éléments de notation
		7. La capacité de bande passante Internet en gigabits par seconde (Gb/s) au Canada Le soumissionnaire devrait fournir les gigabits par seconde (Gb/s). 8. La moyenne quotidienne du nombre de cœurs physiques déployés dans les centres de données énumérés dans l'élément 3 du 1er au 29 février, 2024. 9. Pourcentage de la capacité disponible en termes de cœurs physiques. Le soumissionnaire devrait fournir les données associées au calcul suivant : le pourcentage de la capacité disponible en termes de cœurs physiques est calculé comme suit : [1 - (moyenne quotidienne du nombre de cœurs physiques utilisés dans les centres de données énumérés dans l'élément 3 du 1er au 29 février 2024/la moyenne quotidienne du nombre de cœurs physiques déployés dans les centres de données énumérés dans l'élément 3 du 1er au 29 février, 2024 [élément 8])] * **Notation directe** 10. Le soumissionnaire dispose de documents définissant des mesures de latence et de rendement entre ses régions : oui ou non 11. Le soumissionnaire offre un marché pour les applications tierces : oui ou non Pour les éléments 10 et 11 : Le soumissionnaire devrait fournir les hyperliens.	Pour les éléments 10 et 11, les points seront attribués comme suit : **1 point :** Oui **0 point :** Non